HOUSE OF LORDS

Communications and Digital Committee

Corrected oral evidence: Online Safety Act: additional safety measures

Tuesday 16 September 2025

2.15 pm

Watch the meeting

Members present: Baroness Keeley (The Chair); Viscount Colville of Culross; Baroness Fleet; Baroness Healy of Primrose Hill; Lord McNally; Baroness Owen of Alderley Edge; Baroness Wheatcroft.

Evidence Session No. 2 Heard in Public Questions 38 – 51

Witnesses

I: Andy Burrows, Chief Executive Officer, Molly Rose Foundation; Rani Govender, Policy and Influencing Manager, NSPCC; Baroness Beeban Kidron OBE, Founder, 5Rights Foundation.

USE OF THE TRANSCRIPT

This is a corrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

Examination of witnesses

Andy Burrows, Rani Govender and Baroness Kidron.

Q38 **The Chair:** Good afternoon and welcome to this meeting of the Communications and Digital Committee. I thank our witnesses for joining us today in this session, which will focus on the Online Safety Act. As our witnesses know, Ofcom is currently consulting on introducing additional safety measures into its existing codes of practice under the Online Safety Act. Today, we will examine the proposed new measures aimed at improving protections for children online. This session is being broadcast live and a transcript will be taken; our witnesses will have the opportunity to make corrections to that transcript where necessary. Could I start by asking our witnesses to introduce themselves, starting on my left?

Rani Govender: I am the policy and regulatory manager for child safety online at the NSPCC. Thanks very much for having me today.

Andy Burrows: I am the chief executive of the Molly Rose Foundation. We were founded by the family and friends of Molly Russell after her death in 2017.

Baroness Kidron: I am a Crossbench Peer and I was involved with the pre-legislative committee on the Online Safety Bill, now an Act.

Q39 **The Chair:** Thank you; you are all very welcome. I will start by asking the first question. Can you each give us your overall assessment of the additional measures proposed in Ofcom's consultation?

Baroness Kidron: That is a very big question. It may be best, as I presume we will go into detail, to say that I broadly welcome that Ofcom has answered some questions we had, particularly by putting something forward on live-streaming, looking at the user signals across different platforms and so on.

There is plenty to look at and be pleased with, but the nature of the way in which it is doing it is so incredibly slow and iterative that some of the fundamentals are not being addressed here. Briefly and broadly, I mention things such as safe harbour. If we keep on getting tiny increments of change but leaving the big gap in outcome, thus letting everybody off the hook, the incentive of safe harbour is not to do the best but to do exactly what you are told. That is a big problem for the Act. Also, it has not completely looked at some gaps that we all identified, for example around different experiences for different ages and being more concentrated on risk and outcome than on process. So there are big things that all of us—I am sure that my colleagues will back me up on this—have been asking for but which have not been taken up at this opportunity.

At the outset, let me be really clear: the Act has come in for a bashing over the past couple of months, some of which is misinformation and is not right. We are better in the world for having an Online Safety Act than we were before—I want to make that utterly clear—but that is quite

different from being a little more critical about the rate and scope of progress.

Andy Burrows: Ofcom has described 2025 as its year of action. If this is the showcase of the current framework of the Act and how it is being implemented and delivered, we are underwhelmed.

There are welcome measures in the codes—I welcome any strengthening of the first set of measures to protect children better—but, as Baroness Kidron said, this gradualist approach is slow and reactive. We see measures such as live-streaming being addressed in this second volume of codes, which is primarily a reflection of Ofcom's bandwidth and how it is implementing the Act, rather than starting from the point of tackling harm.

We are also concerned that some measures in these codes risk cutting across and potentially undermining the earlier protection of children code. Ofcom rightly chose forms of non-designated content in previous consultations and put a measure on platforms to ensure that platform algorithms are not recommending content where that content had been detected. There is a substantial gap here because the measures around proactive technology that are being proposed do not apply to NDC and illegal self-harm. That would appear to undercut the previous iteration of the code. Certainly, in our discussions with the regulator when the protection of children code was first launched, we were urged to see it as the first of two consultations, with this being the second one. At the very best, they are not joining up effectively.

Rani Govender: I echo the overall point on being supportive of how Ofcom has recognised the gaps that were raised around the previous consultation; it has acted on those, which is a positive sign. I agree on the concern around the time this takes. I would also pick up on the proactive technology measure, recognising Andy's point about the limitations in terms of what it applies to, but, looking at how it looks to address child sexual abuse, it is a welcome measure.

What is particularly welcome about this measure is that it is not prescribing one or two specific solutions—tools that companies should be using—but is putting the onus back on to the tech companies to do that work, which is where the responsibility should be. They should be the ones looking at where the risk is in their services and what tools are out there to best tackle it. That is the right approach in terms of how Ofcom should be looking at tackling these harms and driving that responsibility on to tech companies to do a better job.

Clearly, there is much more to do on this. Andy has illustrated some areas where we could see this expanded. Generally, knowing the outcomes that we want companies to work towards and having those expectations clear are important next steps, as Baroness Kidron said. Overall, what we are seeing today is welcome, but there is certainly more to build on.

The Chair: Those responses are welcome, but your comments include "gradualist", "slow" and "reactive". Do you see any benefits to that

iterative approach? Can you all say whether you think that it should be changed and that Ofcom is not taking the right approach? Do you want it to speed up?

Baroness Kidron: That is a difficult question because iterative could mean being careful, looking at cultural change, changing the narrative and bringing everyone with you. If that were what iterative meant in this context, we would all be for it. Iterative meaning, "We can do only this bit then that bit", is as much an opportunity for further lobbying, diluting and mismatching—as we heard from Andy—as it is for being careful.

I understand the idea that we are building one code on to the other, but we are not seeing it building the golden future that has been described. That is the problem. Iterative has to mean, "We are all going here. This is what it is going to look like. Don't be impatient, this is step two", but we do not have that horizon in front of us. In fact, the people represented here are constantly saying, "This is our horizon. Are you going to meet it?" Ofcom is not quite willing to have that conversation.

Andy Burrows: In this second iteration of the codes, we are still seeing measures that bake in the current industry response, in essence, rather than incentivising safety by design and taking us beyond what the status quo currently looks like. Let us look at some specific measures that are being proposed in this consultation, such as the user sanctions policy and the use of proactive technology in respect of suicide. Both are welcome and potentially powerful measures, but the way in which they have been drafted focuses on accuracy, rather than accuracy and an articulation of the outcome.

Let us look at the current state of play. Take proactive measures, for example. We undertook analysis based on the Digital Services Act data out of the European Union. We saw that 98% of some 12 million content moderation decisions taken by six major platforms are taken by two of them; 2% of the total content moderation decisions related to suicide and self-harm combines Instagram, Facebook, Snapchat and others. We already have those measures in place. What Ofcom's measures are doing is simply requiring that that is the case; they are not making sure that they reach a certain threshold or standard. When the data is showing us that those measures are already being employed, with wildly divergent results, on platforms that have different functionality but are much of a muchness in many respects, the lack of that outcome focus—and of an articulation of what platforms should be striving for—means that the overall effectiveness of these measures will be blunted.

Rani Govender: I agree with a lot of that. I would add that, if we are seeing this iterative approach—clearly, we all welcome the code being strengthened and built on over time—we have to do the best job we can now in tackling the harms that we know exist. There is a huge amount of evidence and research on where these risks lie and what is enabling them. If we look at how perpetrators operate online, there is more that we could do to attack a decade-old understanding of those patterns of behaviour.

The other solution that we would push goes back to the point around future-proofing. How can we make sure that the measures stand up to a constantly evolving online landscape? We will talk more about emerging harms, but that is why we welcome any approach that puts a responsibility on tech companies to have onerous risk assessments. We will need a lot of transparency around what is in those risk assessments and what companies are doing off the back of them, but they are a crucial lever. It is going to be important to have more code measures that push companies to think consistently about how they should be evolving their own practice and not always waiting for Ofcom.

Q40 **The Chair:** How can Ofcom and, where relevant, the Government keep pace with the latest developments in online harms and technologies? Are they not doing that? Do you have any advice on how they should do it?

Baroness Kidron: That raises something tangential that I am concerned about: we have had a number of debates in the House that identified gaps between what we as parliamentarians thought the Act brought forward and how Ofcom has interpreted it.

The Government could play a useful role in sorting out that gap. For example, at the last minute, Baroness Morgan was successful in making sure that risk as well as size was going to be a factor in categorisation—then it was not. I had something similar around addiction, which, in its own pure terms and not around content, was not adequately reflected. The Government could do a useful job here in saying, "We interpret Parliament as having said X or Y", and making sure that, without encroaching on the independence of the regulator, Parliament's will has been interpreted. The Government could do other things in relation to safety by design and look at safe harbour and so on.

I specifically want to say this because, although we are sounding critical of Ofcom, we must be careful in talking about things we failed to do with the Act that would empower Ofcom; the powers that the current Secretary of State has to make an intervention that would help Ofcom; those things that we are saying, which I am certainly saying, Ofcom could do better; and the things that we very much welcome. We have to see it as different packages of action rather than a single, "Can we catch everything?"

Q41 **Viscount Colville of Culross:** I want to go back to safe harbour; I am slightly confused by it. You are worried. Rani, you talked about how you thought that it allowed companies to respond in the lowest possible way rather than raise their game. Should there be safe harbour? What is the point of it? Do we not want to make sure that the processes and outcomes are as good as possible, and not give them this safeguard? One of the points of the Online Safety Act was to get away from the idea of safe harbour, which we had had for publishers.

Baroness Kidron: I look forward to your recommendations. To be clear, safe harbour has an interesting function if what it does is incentivise a

company to do its absolute best and not be punished for doing so. Safe harbour, as a concept, is interesting.

In the American versions of the age-appropriate design code that I have been involved in, we put safe harbour in as an incentive to say, "If you do everything and something goes wrong, it is okay". The way it has worked in the Online Safety Act is that, if you do Ofcom's 44 measures—or whatever number it is now—you are fine. You can choose to do something different but, if you do, you do not have safe harbour. That is a problem because, if what you could do is different, quicker, better, more advanced, more thoughtful and more nuanced, you could actually not have safe harbour for doing the better thing. That is why we are talking about it as a negative incentive in this instance.

Viscount Colville of Culross: If you do the 44 things that Ofcom tells you to do, you have safe harbour. Anything you then do above that, you still have safe harbour. What is the problem with that?

Rani Govender: One thing I would add, particularly in the context of this question around emerging risks and tools, is that we would expect companies, particularly the large services, to do thorough risk assessments where they gather a lot of data and evidence and genuinely understand what is happening on their service. There are a lot of reasons why they might be a step ahead of the rest of us, because they ultimately have the power to collect that data. If they are spotting new trends and new ways in which harms are developing on their platform, but there is nothing in the code of practice to address them, there is no obligation on them to address those harms. So, when we are thinking about how we stay on top of emerging harms, there has to be something that forces companies to take action immediately once those harms have been identified and to look at what they can do to mitigate them. At the minute, there is no incentive.

Baroness Kidron: Can I add one tiny thing on this? It puts an enormous pressure on Ofcom, because Ofcom always has to be right about what the answer is if it is its measures that give safe harbour. This is a problem because it fixes them in spring 2024 as the perfect time of what was available then. That is a pressure that any national regulator should not be under. It should be pushing the outcomes and determining the floor but not determining the route to get there. That is the heart of the problem.

Andy Burrows: I completely agree; I second that point. The problem we are seeing with safe harbours is not necessarily with safe harbours per se; it is about the way in which safe harbours are working when they are interplaying with the risk-averse approach that Ofcom is taking, resulting in codes that, in effect, reinforce and bake in the status quo.

There is another point that I would make here about the evidentiary threshold. It is about being able to respond and keep pace with emerging and agile technologies and, therefore, agile and evolving threats. Ofcom is applying a high evidentiary threshold, presumably in order to try to safeguard the measures from JR and challenge from industry, but that

creates a challenge because, clearly, we are talking about harms that are evolving at pace. The challenge in generating evidence to meet that threshold means that we have a slow, reactive response.

A specific point I would make is that there are areas where I would be critical of Ofcom's agility in identifying and responding to new harms. One thing that worries us tremendously is the threat posed by com groups—groups of young men being groomed as perpetrators and drawn together by fluid ideologies. We are seeing them commit a whole range of truly appalling harms, including a new type of grooming focused on suicide and self-harm and driven by sadistic behaviours.

I first warned Ofcom of these groups in January 2024. We have seen six advisories from global law enforcement agencies; the FBI recently warned of a sharp increase in the threat. There is still no evidence that the codes have been drafted to account for the risks posed by these groups and, when the register of risks was updated in December, there was only a scant passing peripheral reference to them. As someone who has worked in this space for a decade, I have to say, this is one threat type that I find more disturbing and chilling than anything else I have seen. Law enforcement agencies are queuing up to say, "This is a huge concern". We are starting to see children, particularly girls, being groomed for purposes of self-harm and suicide. These are the most appalling and egregious acts of harm; there are stories of girls being coerced into self-harm acts relating to these groups. I have heard from parents here in the UK who are desperate to see the regulator take action, but some of those risks are not being recognised.

That is not consistent across the piece. On harms such as child sexual abuse, Ofcom is doing a very good job of understanding and articulating the risks, but it is not where it needs to be on these newer harms.

The Chair: Thank you for raising that; that is helpful.

Q42 **Baroness Owen of Alderley Edge:** In your understanding, do you think that it is a capacity issue or lack of horizon scanning on Ofcom's part? Where is the fault line?

Andy Burrows: Some of it is capacity, but a lot is horizon scanning. It feels to me that there has almost been a failure of imagination in conceiving of what suicide and self-harm offences look like.

The regulator has a very good understanding of the way in which algorithmic harm, such as that which contributed to Molly's death, plays out. However, on the nature of offences where we are ostensibly talking about grooming—where we see grooming for the purposes of sexual gratification or financial motivation—there has not been the appropriate horizon scanning for new types of grooming driven by the darkest type of motivations that we can think of: sadistic motivations and a whole melting pot and mélange of harm types. That has then bound the constraints of how Ofcom is viewing the problem.

Baroness Kidron: May I come in briefly on that? It is also closely connected to the idea of what evidence is. There is an argument to talk

to young people, as they will tell you this is happening. Talk to parents and talk to teachers. This idea of classic evidence has not been accompanied by accessing the evidence that sits in the tech companies. I would be interested in how many information notices Ofcom has sent since having the powers; I do not know whether the committee has asked that but, when I checked a few months ago, it was none, even though it had the power. So where is the evidence going to come from? If the evidence is not going to come in a form that Ofcom would like, what other signals is it willing to make because, two years later, we are still without evidence? I put on the record that, thanks to Viscount Colville, we got research access during the passage of the data Bill, which was very important.

The Chair: Thank you, both, for raising that; it is very helpful. Thank you, Charles, for doing that.

Q43 **Baroness Fleet:** Thank you so much for coming; we really appreciate it. I know how busy you all are. You are absolutely steeped in this subject.

We have seen a real lack of public trust in age verification. People are very aware of the whole issue of VPNs. Do you think that what Ofcom is now proposing—to extend the age verification—will actually work? Do you think that Ofcom has learned lessons from the first stage? It overlaps a little with what you have been saying, but can you see any benefits in using HEAA to target child safety settings at child users, as opposed to applying them to all users? Where would you draw the line on that?

Baroness Kidron: I might try to tackle the, "Have they learned the lesson from the last round?", piece of your question.

I had a Private Member's Bill on the subject of age verification a few years ago; a great deal of it was moved into the Bill and is part of the Online Safety Act. The one bit that was not adequately reflected—there is a great deal of evidence in *Hansard* that we discussed this ad infinitum—was the question of privacy. I remember standing in the Chamber and saying, "It will never be acceptable to the adult population if age assurance is not radically private and if that is not at the core".

I will say—I do not want to misspeak here because Ofcom says that it should be privacy protecting and must meet the ICO codes—that it is all very roundabout. One thing I would like to know—I will write to Ofcom—and which the committee might like to consider, is: what happens when people are introducing age assurance in a way that is not privacy preserving? If someone is asking for a driving licence or a passport unnecessarily, or if someone is asking for more data than is required to establish age, that is going to undermine fundamentally people's sense of safety in the information that they give—particularly, let us face it, male adults who are trying to access pornography, because they do not necessarily want the social embarrassment. What I would now like to see is a recommitment on privacy. I would also like to see Ofcom use its powers to say that, where it is not privacy preserving, age assurance has

not met the bar of being highly effective because it is not highly effective in a cultural sense, even if it determines whether or not you are 18.

I have some more complex views about whether it should be 18 or why it is not doing "age-appropriate" more generally, but, in answer to your specific question, unless we get the privacy right, we will never get proper acceptance of this idea.

Q44 **Viscount Colville of Culross:** I want to try to pin you down, particularly after you spectacularly failed to get an answer yesterday on your question; it was a dismal session.

You talk about the importance of pinning down privacy when it comes to age verification, but I am still not absolutely clear on what details you want. There is a privacy provision with age verification, when you go on to most sites where there is thought to be a risk and need for the age verification, is there not? What is extra? What are the details of what you want to happen to make sure that that data, given up by adults who have to pass through age verification, can be kept private?

Baroness Kidron: There are two parts to it. On paper, we are probably closer to my position than not, but it should be a requirement, written down in the code, that data used for the purposes of establishing age may not be used for any other purpose and that, when checking age, you must not check other things such as location or gender.

Assuming that that is the understanding of what data minimisation is, you then have to question whether the companies are doing it. There is a lot of misinformation out there—that is the bit I cannot speak to—saying, "I don't want to give my passport to access this, that and the other". It should not be necessary to show your identity—only the signals of age. There are very good ways of doing it, and there will be increasingly good ways of doing it.

I would be happy to write to the committee outlining some age assurance methods that work, that are privacy preserving and so on. I will not detain you with it right now, but this is a core thing: is it required, and, if it is, is it being implemented?

The Chair: Veronica, we come back to your original question.

Baroness Fleet: That is fine, because it all links in together; you have covered the points very well. Andy or Rani, would you like to add anything?

Andy Burrows: I would briefly build on Baroness Kidron's point about it being up to Ofcom to take enforcement action against not only platforms that have not introduced any form of age assurance but platforms that have not met highly effective age assurance, whether that is through the privacy lens or other characteristics. There was always going to be a sea of controversy and misinformation this summer; that was inevitable. Some examples of how age assurance mechanisms could be fooled were identified in the first few weeks, such as by using an avatar photo; that

raises questions to me on whether a highly effective measure is being deployed.

I would like to see Ofcom act quickly because public trust here is precious. Clearly, privacy-preserving mechanisms are needed; we know that they exist. Enforcement is now the best way of being able to demonstrate to the public that this can be done and that, where we have seen high-profile examples that have generated public concern, it is a reflection on whether we have seen compliance rather than, as it has been framed, whether it can be done.

Rani Govender: I echo much of that. I will take the other part of the question—extending the use of HEAA and applying it to different settings. Recognising all the challenges that we face, highly effective age assurance will have to play a role in the new regime. We cannot give children enhanced protections if we cannot identify who they are, so we have to get it right; we have discussed that a lot.

In terms of applying it to particular safety settings—or not—clearly, there is a benefit in the universal application of these safety settings because it means that, at whatever age a child might have managed to create their account, whether that is a child or adult account, they will benefit from these settings because they will be everywhere. However, there are real trade-offs to this as well.

Take the grooming settings that are being looked at in terms of having age assurance applied to them: they are part of a two-track approach to tackling grooming. We have the settings and the requirement for services to share user support information at key stages—for example, when a child goes to turn off a setting or first gets a message from a new contact online. That user support is no panacea and will not solve everything, but it has been recognised as an important part of Ofcom's approach. If companies cannot identify children, they cannot tailor that information so that it is age-appropriate, speaks about risks that children face and signposts them to the right kinds of child-specific services.

We should be agile and take different approaches where we can, but it is really important that we do so in a safe, proportionate way. Proportionality is important. Users will not have the option to turn some of these settings, such as the live-streaming ones that we will come on to, on or off; they need to be on for children, and they need to be unable to change them. Age checks are right for children, but you might ask whether it is also proportionate for adults to have settings that children must have. There will be compromises in a lot of this. These are discussions that we must keep on having but, from our perspective, age assurance will be a really important part of that.

Q45 **Baroness Fleet:** Andy, you mentioned that Ofcom must take action. Are you aware of it limbering up to take action? Is it actually taking action, or is it just talking about taking action? Are you aware of platforms that are already under investigation and being put on the spot?

Andy Burrows: Ofcom has said that it has launched several dozen investigations, primarily, I believe, against sites that have not complied at all. Most of those have predominantly focused on small pornography companies, not other services where we have seen reasonable questions around whether the highly effective threshold has been met. A lot of this may take place through supervision—clearly, that is a relatively opaque process; we are not privy to what activity is taking place—but public proactive enforcement is a great way of resetting the narrative and tackling some of the misinformation that we have seen here.

Q46 **Lord McNally:** To understand where Ofcom is in all this, are you saying that Ofcom should be maximising and seeking to test its powers? With any regulator, there is always the danger that, if it does so, it will be accused of overreach and such. Where in the implementation of these powers does the responsibility of Ministers lie? There is always a danger with legislation that, once it is passed, the caravan moves on. If you go to a Back-Bench MP, they will say, "But we dealt with that in the Online Safety Act". You are now saying that there are lots of holes. How much do you think Ofcom has the bottle and desire to stitch up those holes?

Andy Burrows: The reality is that we will see the platforms try to pursue legal challenges, whatever Ofcom does. I would hope that the message the new Secretary of State is giving to Ofcom's chief executive is that it should be trying to use its powers in the most muscular and assertive way, sending a signal to industry that it intends to enforce the powers available to it robustly. If you contrast Ofcom's approach so far with that of the European Commission and its enforcement of the DSA, say, the public messaging has been very different. So far, I do not get the impression that companies are quaking in their boots at Ofcom's enforcement approach. Some of that may be taking place under the guise of supervision, as I say, but that is an incredibly opaque process so it is difficult to conclude whether it will be effective or is sufficiently industrious.

Baroness Kidron: On this issue of age assurance, Ofcom has the power. It should be insisting that highly effective is highly effective; that privacy is a core concern; and that it is working with the ICO to deal with it for reputational reasons. Only at the point at which it hits a block and says, "We cannot enforce against this", is it a ministerial problem. So this specific piece is in Ofcom's purview right now. I recognise that Ofcom intends to embed the right of appeal on age assurance in illegal codes just as it did in the children's code, which is, to be clear, very welcome and a good idea.

Your broader point, I think, is that, unless Ofcom tests its powers, it cannot turn to Ministers and say, "Do you know what? You got that wrong". In defence of Ofcom, the Act is wrong in places, leaves certain gaps and needs more work. When we industrialised, we had 17 Factory Acts, not just one. This is a new area of industrialisation, and we will have more. The frustration is that, where it is clear and mandated, we do not want to see Ofcom stroking platforms and saying, "Come on, guys, do it". We want to see it taking action and being robust. I am

sympathetic anywhere where Ofcom feels it needs a power but that has not been provided by Parliament.

The Chair: I am aware of the time; we should move on to our next question. Rani, do you want to make a point as well?

Rani Govender: No; I am happy with all that.

The Chair: Thank you for those responses.

Q47 **Baroness Healy of Primrose Hill:** The committee is concerned about live-streaming, especially as Ofcom states that the majority of CSAM identified by the Internet Watch Foundation derives from content captured from children's live streams. Are the proposed safeguards around live-streaming adequate to protect children?

Rani Govender: We welcome the fact that Ofcom has heard civil society's concerns around the risks in live-streaming and introduced these measures. Safety settings on children's accounts are really welcome. When we look at those functionalities, there is a clear evidential link to CSA, grooming, coercion and other forms of harm, such as the harassment and bullying of children online. These measures are incredibly welcome steps forward, but there will always be more to do and more that we can do.

We will come on to the point about minimum ages for live-streaming, which I am happy to talk about, but the other point I want to raise is that these settings will be on children's accounts when they host one-to-many live streams, not many-to-many. Many-to-many can sound confusing, but that could literally be two child users on their individual accounts collaborating to host a live stream jointly; all of these welcome protections will not be there. That is clearly a gap and a loophole. It is a very easy way in which anyone determined not to have these protections could get around them.

I recognise that Ofcom thinks that there is a challenge because many-to-many can also mean lots of people live-streaming to one another at once; in a gaming environment, that looks very different to in other services. We are not saying that it has to mirror the approach in every scenario, but one of the urgent next steps is to look at that gap.

Andy Burrows: I applaud Ofcom for the measures it has taken. It is building in some welcome aspects of friction. The restrictions around children being able to comment on, react to or screenshot a children's live stream are welcome, but I would like to see more upstream measures. For example, I cannot see a credible case for algorithmically recommending the live stream of a child, which is integral to the design of TikTok. Measures around the reporting of imminent physical harm are, again, a welcome step, but, in respect of suicide, only the act of suicide is covered; they do not cover self-harm or dangerous stunts. I would think that, by any reasonable understanding, those would be considered an imminent physical harm, so I cannot understand the discrepancy there.

A broader point I would make—this is a function of the Act, not Ofcom's implementation of it—is that the focus on live-streaming is great but look at private services: 50 people can join a call on Messenger, 32 on WhatsApp and 25 on Discord. As long as the code is not applied to private message services, there is the risk that, even where we are seeing welcome steps on public services such as live streams, they will just migrate to private channels. Where does a live stream stop and a group chat end, if you are thinking about 50 people on there? In respect of the com groups I talked about earlier, you can see how likely it is that, with organised CSA, you would see some migration there.

Baroness Kidron: I second what has been said by my colleagues here. I am absolutely delighted that this has been given such a focus.

First, I wanted to say something detailed on flagging. Any kind of flagging should be possible without being in-app, on the service or logged on in any way. Flagging that is possible only in services is a perennial issue; you may be a parent or a teacher, and someone may have just told you, so you need to be able to alert. I have had a particularly torturous and ongoing experience with Meta. We tried to flag this and to alert it; its lawyers wrote to us and said that abuse@meta.com is not a monitored email. I would like to know that flagging and alerting mean alerting.

Secondly—I am not going to pretend to be an expert in this—I would caution on the requirement around human moderators. This speaks again to what we were talking about: outcomes versus process. I do not care how anybody works out that something is going wrong; the outcome must be that, when it is going wrong, it is found and dealt with. I do not know why a human being is necessarily better than an automated solution. Where it is, it should be used; where it is not, it does not matter. So, again, let us not worry about the process—let us fix on the outcome.

Q48 **Baroness Healy of Primrose Hill:** Should children be prevented from live-streaming altogether? Should there be age brackets at different points under the age of 18?

Rani Govender: It is not a proposed measure yet, but we welcome the fact that Ofcom is open to thinking about it. The next step with regulation should be thinking not just about adult versus child experiences but about how we can ensure that children have age-appropriate experiences that consider their stages of development and so on. There is a really strong case for applying that to live-streaming.

We propose that setting a minimum hosting age of 16, certainly on social media sites, would be proportionate. If we look at the evidence, the huge risk that younger children face on live-streaming is abundantly clear. Ofcom's profiles of how children in different age groups behave online show that the 10-to-15 age group is particularly likely to be impulsive and take risks; that is a concern when it happens in live-streaming environments.

We also know from the IWF's data that, in the production of child sexual abuse material, younger children are particularly at risk. The NSPCC research from a few years ago showed that children of primary school age are disproportionately more likely to be asked to remove clothes on live-streaming. So, it is clear that live-streaming is far from a "safe by design" experience for children at the minute.

We welcome these measures coming in but, given the scale and immediacy of the harm that we can see in these environments, it makes sense to raise the minimum age to 16; to make sure that 16 and 17 year-olds still have really strong protections; taking proactive steps, implementing these settings and looking at how it can be made safer. This is certainly somewhere where we can start to take that tailored approach.

One thing I would like to add is that, generally, there have been lots of debates about children's access to the online world and blanket increases to minimum ages. I do not think that that is appropriate. Children can get a huge amount of benefit from being online, and they have a right to enjoy that, but we must look at where the harm is too extreme and too significant and put in sensible age limits so that we are not stopping them getting most of the benefits that they get from the rest of the online world.

Andy Burrows: I agree with everything that Rani has said. If platforms want to offer live streams to children, they should be taking further steps above and beyond the regulatory requirements to demonstrate that it can be done safely. I spoke in my previous answer about TikTok, for example. The "For you" page's algorithm recommends live streams. Many of us will have seen circumstances where there is a child who ostensibly looks quite vulnerable but is being algorithmically recommended. I cannot see how that is consistent with the fundamental principles of safety by design. If the platforms cannot take those steps, we absolutely should be looking, as Rani says, at a functional-based application of minimum age points where we can turn those features off and on.

Baroness Kidron: I was very interested to hear your witness last week talk about putting in a delay for children. I have not thought about that in great detail, and I do not know the research, but it is a really interesting idea that should be unpicked. I think that, for very young children, it is completely inappropriate. It is disappointing that Ofcom did not pick up the various places in the Act where it said "age-appropriate"; something is completely different for a 12 year-old, a 14 year-old or a 17 year-old. I would be horrified if live-streaming were not available to 17 year-olds, because it seems to be something that they should be able to do, but we have to come back to this idea of judging companies on the outcome. If the outcome of a 17 year-old live-streaming is that it is safe, reasonable and not dangerous, bring it on, say I—but, if it is not, it is a dangerous product. Why are we giving it to children? I would like to see a lot of more of that thinking as we move forward with the online safety regime.

Andy Burrows: May I briefly add a fundamental and oft-visible point on the lack of measures being articulated around outcomes? When you look at the measures around live-streaming, a requirement to have human moderators is great, but what is the outcome? A requirement to have a report is great, but what do companies need to do when that reporting function is triggered? We are already seeing the ambiguity in Ofcom's drafting being exploited. We issued research a couple of weeks ago analysing social media platforms in the weeks before the Online Safety Act took effect. We started to see some measures in Ofcom's code be rolled out ahead of time, but the ambiguity in the drafting was being exploited.

One of the measures in the protection of children code is that there should be an opportunity for children to offer negative feedback on content being algorithmically recommended to them. If it is implemented well, that is a fantastic step that can give children better agency over their feeds, but the way in which both Instagram and TikTok have implemented it is that you can say not only, "I'm not interested in this type of content", but, "I am interested in it", which results in you being served further similar content for the next 30 days. We saw repeated examples of suicide, self-harm and intense depression-related material where that ambiguity was being exploited and children were being served more of that content. Outcome-based articulation of what companies need to do is fundamental.

The Chair: I want to move on to Charles's question. We are quite short of time now.

Q49 **Viscount Colville of Culross:** This is the final set of questions. In our session last week, we heard about the use of proactive technology such as hash matching. Do you think that it should be rolled out to analyse user-generated content that is communicated privately? Would it be able to pick up on hints to signpost perpetrators of illegal content communications? Andy, do you have anything to say about that?

Andy Burrows: I would say yes. This argument often generates a huge amount of heat rather than light, to say the least. Well-known experts in the field, such as Professor Hany Farid at Berkeley, would say that it can be done without breaking encryption. It is a hugely powerful tool.

When you look at the research on CSA done by Professor Michael Salter out of Australia, you can see that, with private chats, CSA offenders are more likely to use certain platforms by a factor of, in some cases, 20 or 30 times. If hash matching can be done and is technically feasible, it absolutely should be done.

Rani Govender: I echo that entirely. I would add that we know that an absolutely fundamental part of the grooming pathway is, typically, starting communication with children in more public, open forums—gaming platforms and so on—then moving these communications into private spaces. Although it is welcome that the proactive technology measures will be implemented in public spaces—to be clear, this is a limitation in the Act, not Ofcom—if they are not being used in private

spaces, we are not using the solutions where they are actually needed and we are continuing to rely on children to defend themselves.

The core of the Act was that we all accepted that the burden has been on children for far too long and that things need to change, but, if there is harm—I can only see how it would increasingly migrate to these private spaces as the public spaces get, I hope, safer—that is unacceptable. Ofcom has powers that it can use in specific circumstances; it should go as far as possible with those to compel private companies to act. Again, as we were saying, where it bumps up against the legislation and cannot go any further, that is something the Government will have to consider.

Baroness Kidron: I agree with what has already been said. The only thing I want to add is that I have a particular bugbear: Ofcom has rightly stopped direct messaging between unknown adults and children but has not stopped friend requests. So an unknown adult can make a friend request and, if the child answers it, they can then direct message. This issue of how you fish for children in the public arena then take them into private spaces cannot be a place to hide.

Q50 **Viscount Colville of Culross:** How should platforms handle cases where children themselves upload CSAM? If children start sharing this content, should they be banned completely without exception? Are there any problems with doing that?

Baroness Kidron: This is probably one of the most difficult areas for me, because not everything that is happening in relation to that is completely innocent. There are some very aggressive, purposeful and intentional things that people under the age of 18 are doing to each other or to themselves. You cannot just go, "Oh, they're kids, it doesn't matter".

I am involved in a case with a child of 13 who forwarded a Snapchat sticker that reached the threshold. There have been months of legal horror with the CPS, in terms of whether it is going to charge him and so on. I would say that criminalising children is the absolute last resort; culturally and educationally, we need to put a lot more resource into trying to help children understand why some of the things that they are doing are not appropriate and not right.

All of the things that we are talking about—safety by design, amplification and nudging kids into these behaviours—will have an impact on how many of these kids are doing that and on some of the com groups that are pushing this behaviour. There is a fine line between victims who are doing the wrong thing, perpetrators who are doing the wrong thing, innocent wrongdoing and some messy things in the middle, which are probably the most difficult thing to legislate for. We should have a policy that criminalises children only as an absolute last resort; I would like to see more education and rehabilitation in that space.

Q51 **Viscount Colville of Culross:** Prior to criminalising, is banning those children from the digital space satisfactory?

Baroness Kidron: It is difficult to know what banning means: how far, how long, from what and for what purposes? You have to remember that children's lives are very complex. It depends on what you are banning them from. There are many ways in which they need to access not a specific service, perhaps, but—

Viscount Colville of Culross: You could ban them from a specific service, could you not, if that is the service on which they exchanged CSAM?

Baroness Kidron: You could, but I would like to see a slightly more tolerant "Three strikes and you're out" approach, unless it is intentional. I would like to see something much more educative and careful in this arena. Children feel bereft at being excluded; one thing that does not come up in these conversations about online safety is the cry from children about what else is on offer. They cannot go in the street. They do not have parks. They do not have after-school clubs. The children I engage with speak about being kettled into the digital world. If you then exclude them from certain spaces, that is a punishment upon a punishment. So we have to be careful on this particular issue.

Viscount Colville of Culross: What about you, Rani? Do you agree? Do you think that banning is something that should not be considered in these particular cases because it would be kettling upon kettling?

Rani Govender: Yes. First, in all scenarios at the NSPCC, we want children to be met with that safeguarding response. If we just leap into bans, that scares children away. We want to make sure that we are never deterring children from speaking up about something that has happened to them, whether that is something they have experienced or something they might have done online. Those principles have to be at the front of our minds.

It is important to be clear that one option Ofcom is currently considering is permanent bans on children, including children who are victims of grooming and online abuse.[1] To us, that is absolutely unacceptable. We must be clear that there must be no form of victim-blaming at all in these final proposals. Baroness Kidron made an important point: lines can be blurred around exactly what has happened. I am personally not comfortable with the idea of tech companies being the arbiter on what has happened to children and making those extremely sensitive decisions. So, for us, permanent bans for children have to be out of the question.

Where there has been real harm and there is a clear understanding of that—perhaps coming from reports from other children that clear harm has taken place—it is worth saying that a group of young people with which the NSPCC works on online safety has proposed something similar to a shorter-term suspension or a strike-based system. They do not think

[1] Note by the witness: The witness would like to clarify that whilst this is one of the three options Ofcom has included in its consultation, the consultation document also indicates that Ofcom will not pursue this option because it is seeking an approach which is "not punitive of child victims and survivors".

that there should never be any consequences, but it is important that those consequences are proportionate. From a youth justice perspective, we would not impose the harshest measures on children as we might sometimes do with adults; if we are saying that permanent bans are suitable for adults, it does not mean that we should just copy them on to children. So I would like to see an alternative proposal from Ofcom on this.

Viscount Colville of Culross: Andy, do you have a different view?

Andy Burrows: I would largely agree. There has to be a high threshold before considering a ban—perhaps at the point where we have arrangements in place and where the CPS may consider prosecuting a child. In the vast majority of cases, it would not be in the public interest to do so; that is the right balance. Any threshold would need to be set very high.

Viscount Colville of Culross: Thank you very much indeed.

The Chair: Thank you; that is very useful. We have had a few sessions. Next, we have a session with Melanie Dawes of Ofcom, so it is useful to be able to run through this. We will reflect back to Ofcom what has emerged from this very short look at these codes of practice. Thank you very much indeed for your time.